

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI**

Maxwell Klassen, *individually and on behalf
of all others similarly situated,*

Plaintiff,

v.

Navvis & Company, LLC d/b/a Navvis,

Defendant.

Case No. 4:24-cv-00035

JURY TRIAL DEMANDED

PLAINTIFF’S CLASS ACTION COMPLAINT

Plaintiff Maxwell Klassen (“Plaintiff”) brings this Class Action Complaint against Defendant Navvis & Company, LLC, d/b/a Navvis (“Navvis,” or “Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to his own actions and his counsel’s investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard protected health information (“PHI”) including, but not limited to, Plaintiff’s and Class Members’ names, dates of birth, diagnosis/clinical information, health insurance policy-related numbers, medical dates of service, medical provider name, medical treatment/procedure information, patient account numbers, and subscriber IDs, and, in some circumstances, Social Security numbers (collectively, “Private Information”).

2. Defendant Navvis is in the business of creating and managing electronic data management software used by health plans, systems, facilities, and professionals to store or transmit Private Information.

3. During the course of its business operations, Defendant acquired, collected, utilized, and derived a benefit from Plaintiff and Class Members' Private Information. Therefore, Defendant owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, including to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach.

4. On or around July 25, 2023, Defendant identified suspicious activity on its computer network environment. After learning of the incident, Navvis immediately launched an investigation to determine the nature and scope of the incident.¹

5. As a result of Defendant's data security failure, over the course of thirteen days, occurring between July 12, 2023 and July 25, 2023, an unauthorized third party was able to access and potentially obtain data containing Plaintiff and Class Members Private Information from its systems (the "Data Breach").²

6. Despite learning of the Data Breach on or about July 25, 2023, Defendant did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until December 29, 2023, more than five months after it discovered the Data Breach.

7. Based on the Notice of Data Breach Letter, Defendant admits that Plaintiff's and Class Members' Private Information was unlawfully accessed and may have been exfiltrated by a third party.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class

¹ *Notice of Data Event*, Navvishealthcare.com, <https://navvishealthcare.com/privacy-update> (last visited Jan. 7, 2024).

² *Id.*

Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

9. Upon information and belief, Defendant maintained the Private Information in a negligent manner. In particular, the Private Information was maintained on computer systems and networks that were in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant; and, thus, Defendant was on notice that failing to take appropriate protective measures would expose and increase the risk that the Private Information could be compromised and stolen.

10. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. The exposed Private Information of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web, as is the *modus operandi* of cybercriminals.

11. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information.

12. Plaintiff and Class Members reasonably expected Defendant to keep their Private Information confidential and securely maintained, to use the information for business purposes only, and to make only authorized disclosures of this information.

13. Because of the Data Breach, Plaintiff and Class Members now face a current and ongoing risk of identity theft or fraud.

14. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class

Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited five months to report it to affected individuals.³

15. As a result of this delayed response, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

16. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendants' inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

17. As a result of Defendant's unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk

³ *Id.*

and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information.

18. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendant’s data security systems, and future annual audits.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, (iv) breach of fiduciary duty; (v) invasion of privacy; (vi) unjust enrichment; (vii) promissory estoppel; and (viii) declaratory judgment.

PARTIES

20. Plaintiff Maxwell Klassen is a Citizen of Illinois residing in St. Clair, Illinois. Plaintiff received a letter dated December 29, 2023, from Defendant Navvis notifying Plaintiff that Defendant’s network had been accessed and Plaintiff’s Private Information may have been involved in the Data Breach.

21. Defendant Navvis & Company, LLC, d/b/a as Navvis, is a limited liability company organized under Delaware law with its principal place of business located at 555 Maryville University Drive, Suite 240, St. Louis, Missouri 63141. Defendant can be served at its principal place of business via its registered agent, Adam Schneider.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

23. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

The Data Breach

25. In the ordinary course of its business, Defendant receives, stores, maintains, and uses Plaintiff and Class Members' Private Information, including but not limited to, their names, medical treatment information, and in some cases, Social Security numbers.

26. Given the sensitive nature of the Private Information in its possession, Defendant knew, or should have known, the importance of securely storing and maintaining Private

Information on its network.

27. On or about July 25, 2023, Defendant discovered its network had been breached by an unauthorized individual as far back as July 12, 2023.

28. Following a forensic investigation, Defendant then discovered that unknown cybercriminals had accessed, obtained, and potentially exfiltrated the Private Information of Plaintiff and Class Members.

29. Defendant's Notice of Data Breach admits that Plaintiff's and Class Members' Private Information was accessed without authorization, and states that although it knew of the Data Breach as early as July 25, 2023, it waited until December 29, 2023 to begin mailing Notice to affected individuals.⁴

30. Defendant further admits that cybercriminals not only viewed and accessed Plaintiff's and Class Members' Private Information, but also acquired it from Defendant's network, meaning the Private Information was exfiltrated.⁵

Defendant's Privacy Policy & Promises

31. Defendant made expressed and implied promises related to its duties and obligations to protect the data it acquired and stored on its system. These promises are incorporated into the Defendant's Terms and Conditions ("Privacy Policy").⁶

32. Defendant's Privacy Policy "recognizes that the privacy of your personal information is important."⁷ Defendant states that it shares Private Information with "third parties who perform functions or services on [its] behalf as outlined in this Privacy Policy and otherwise

⁴ *Id.*

⁵ *Id.*

⁶ *Terms and Conditions*
<https://www.navvishealthcare.com/legal/#:~:text=We%20collect%20and%20may%20use,service>
(last visited January 8, 2024).

⁷ *Id.*

as permitted by law.”⁸

Plaintiff Maxwell Klassen’s Experience

33. As a requisite to receiving medical services from his medical provider, Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law. Upon receipt, Private Information was entered and stored on Defendant’s network and systems.

34. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

35. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendants failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

36. The Notice Letter dated December 29, 2023, from Defendant Navvis notified Plaintiff that its network had been accessed and Plaintiff’s Private Information may have been involved in the Data Breach, which included Plaintiff’s names, dates of birth, diagnosis/clinical information, health insurance policy-related numbers, medical dates of service, medical provider name, medical treatment/procedure information, patient account numbers, and subscriber IDs.

37. Furthermore, Defendant directed Plaintiff to take certain steps to protect his Private Information such as “review[ing] [his] account statements and credit reports for suspicious activity and errors.”

⁸ *Id.*

38. As a result of the Data Breach and Defendant's Notice of Data Breach, Plaintiff heeded Defendant's warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent, in part, at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to review his account statements.

39. Even with the best response, the harm caused to Plaintiff cannot be undone.

40. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

41. He also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

42. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

43. Plaintiff has suffered imminent and impending injury arising from the imminent and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

44. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

45. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable

46. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

47. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

48. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."⁹

49. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.¹⁰ The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

⁹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last accessed Aug. 23, 2021).

¹⁰ See 2021 Data Breach Annual Report, 6 (ITRC, Jan. 2022) available at <https://notified.idtheftcenter.org/s/>.

51. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹¹

53. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹²

54. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Value of PII and PHI

55. The PII of consumers remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity

¹¹ FBI, Secret Service Warn of Targeted, Law360 (Nov.18,2019), <https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware>.

¹² See Maria Hernandez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹³ According to the Dark Web Price Index for 2021, payment card details for an account balance up to \$1,000 have an average market value of \$150, credit card details with an account balance up to \$5,000 have an average market value of \$240, stolen online banking logins with a minimum of \$100 on the account have an average market value of \$40, and stolen online banking logins with a minimum of \$2,000 on the account have an average market value of \$120.¹⁴ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁵

56. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

57. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information...[is] worth more than 10x on the black market.”¹⁶

58. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

59. The fraudulent activity resulting from the Data Breach may not come to light for

¹³ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

¹⁴ *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at: <https://www.privacyaffairs.com/dark-web-price-index-2021/>

¹⁵ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

¹⁶ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Aug. 23, 2021).

years.

60. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”

61. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

62. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

63. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁷

64. As such, future monitoring of financial and personal records is reasonable and

¹⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 23, 2021).

necessary well beyond the one year of protection offered by Defendant.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

65. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

66. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

67. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁸

69. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen,

¹⁸ See generally *Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., <https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business> (last accessed May 1, 2023).

fraudulent use of that information and damage to victims may continue for years.

70. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁹

71. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up

¹⁹ *Id.* at 3-4.

for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....²⁰

72. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

²⁰ See Security Tip (ST19-001) Protecting Against Ransomware (Apr. 11, 2019), *available at* <https://us-cert.cisa.gov/ncas/tips/ST19-001>.

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].²¹

73. Moreover, given that Defendant was storing the Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

74. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

75. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

76. Because Defendant failed to properly protect and safeguard Plaintiff and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system files and exfiltrate that data.

Defendant Failed to Comply with FTC Guidelines

77. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision

²¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

making.

78. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.²²

79. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

80. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their

²² Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>

data security obligations.

82. Upon information and belief, Defendant failed to properly implement basic data security practices.

83. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

84. Defendant was always fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

85. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

86. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

87. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

88. Upon information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

90. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

91. HIPAA requires covered entities and business associates of covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

92. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

93. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

94. A Data Breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI that is not permitted under HIPAA.

95. A breach under the HIPAA Rules is defined as, “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. 164.40.

96. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. *See* the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. *See* 45 C.F.R. 164.308(a)(6).²³

97. Defendant’s Data Breach resulted from a combination of insufficiencies that demonstrates Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant’s Negligent Acts and Breaches

98. Defendant participated and controlled the development, implementation and enforcement of its privacy policy and controlled the process of gathering the Private Information from Plaintiff and Class Members.

99. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff

²³ *See* <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> at 4.

and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiff and Class Members and/or were otherwise negligent because they failed to properly implement data security systems and policies for its health providers network that would adequately safeguarded Plaintiff's and Class Members' Sensitive Information. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

- a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members Sensitive Information;
- b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;
- c. Failing to test and assess the adequacy of its data security system;
- d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- e. Failing to put into develop and place uniform procedures and data security protections for its healthcare network;
- f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- h. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- i. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports

in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

- k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- l. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption).
- p. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;
- q. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;
- r. Failing to implement or update antivirus and malware protection software in need of security updating;
- s. Failing to require encryption or adequate encryption on its data systems;
- t. Otherwise negligently and unlawfully failing to safeguard Plaintiff’s and Class Members’ Private Information provided to Defendants, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

100. As result of Defendant’s ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

101. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) “out of pocket” costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant’s possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

102. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

103. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

104. For example, armed with just a name and date of birth, a data thief can utilize a

hacking technique referred to as “social engineering” to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

105. The dark web is an unindexed layer of the internet that requires special software or authentication to access.²⁴ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or ‘surface’ web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address is ciadotgov4sjwlzihbbgxng3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.²⁵ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

106. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PHI at issue here.²⁶ The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security

²⁴ Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁵ *Id.*

²⁶ *What is the Dark Web?*, Microsoft 365 (July 15, 2022), <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

numbers, dates of birth, and medical information.²⁷ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”²⁸

107. Theft of PHI, in particular, is gravely serious: “A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²⁹

108. One such example of criminals using PHI for profit is the development of “Fullz” packages.

109. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

110. The development of “Fullz” packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and

²⁷ *Id.*; Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁸ *What is the Dark Web?*, Microsoft 365 (July 15, 2022), <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

²⁹ See Federal Trade Commission, Medical Identity Theft, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Sep. 13, 2022).

Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

111. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.³⁰

112. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."³¹ Defendant did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

113. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

114. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

115. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

³⁰ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> (last visited Oct. 21, 2022).

³¹ *Id.*

116. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”³²

117. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.³³

118. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers’ finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.³⁴

³² Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited May 28, 2015).

³³ See generally <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

³⁴ See, e.g., <https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices> (last accessed: October 21, 2022).

119. Defendant’s failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff’s and Class Members’ injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

120. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

121. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant’s Notice instructs them, “review[ing] health care statements for accuracy and report to your provider or insurance carrier any services or charges that were not incurred.”

122. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

123. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in

which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁵

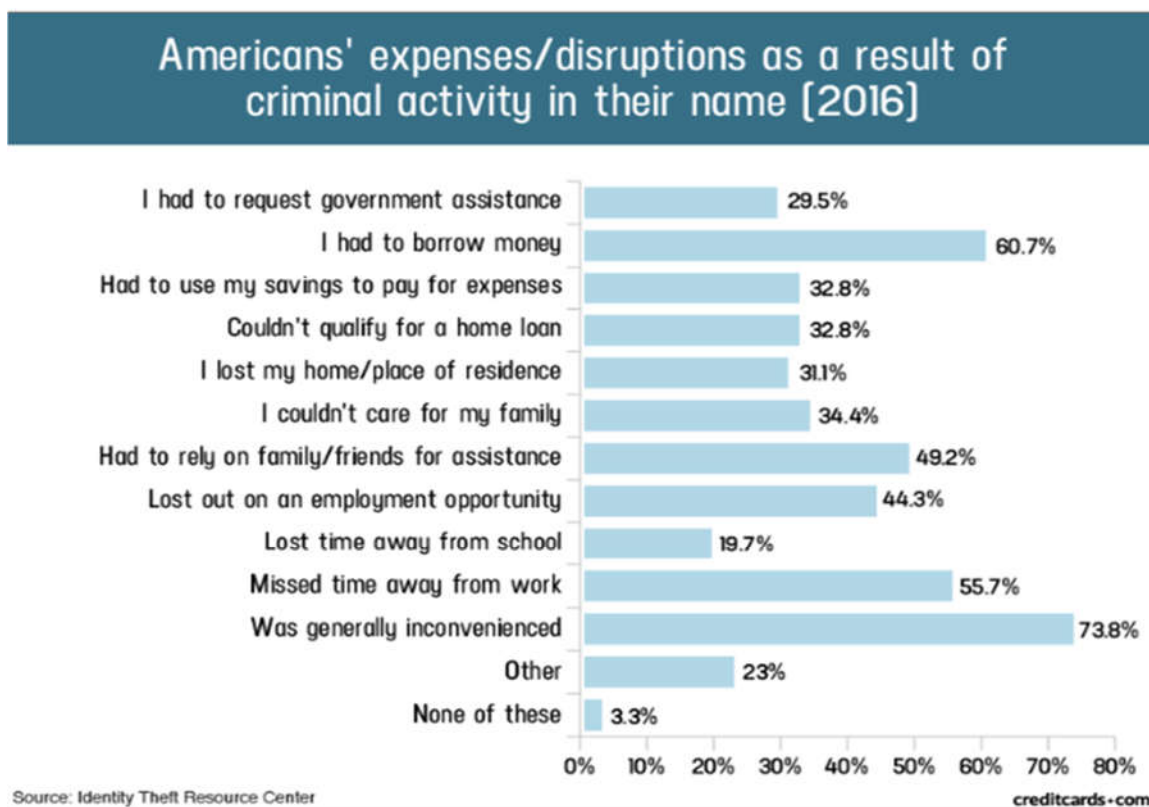
124. Plaintiff’s mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁶

125. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:³⁷

³⁵ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁶ See Federal Trade Commission, Identity Theft.gov, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

³⁷ Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 24, 2017), <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.



126. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁸ Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁹

³⁸ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

³⁹ See <https://www.identitytheft.gov/Steps> (last visited Sep. 13, 2022).

Diminution of Value of the Private Information

127. PHI is a valuable property right.⁴⁰ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

128. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

129. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.⁴¹

130. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for \$50 and up.⁴²

131. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴³ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

⁴⁰ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

⁴¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

⁴² <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last visited Sep 13, 2022).

⁴³ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

broker who in turn aggregates the information and provides it to marketers or app developers.^{44,45} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁶

132. As a result of the Data Breach, Plaintiff and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary

133. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach – Defendant has only offered 12 months of inadequate identity monitoring services through IDX, despite Plaintiff and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any other relief or protection.

134. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

135. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong

⁴⁴ <https://datacoup.com/>.

⁴⁵ <https://digi.me/what-is-digime/>.

⁴⁶ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faen.html>.

probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

136. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.⁴⁷

137. Such fraud may go undetected until debt collection calls commence months, or even years, later.

138. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁴⁸ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

139. Consequently, Plaintiff and Class Members are at a imminent and ongoing risk of fraud and identity theft for many years into the future.

140. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants’ Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant’s failure to safeguard their Private Information.

⁴⁷ See GAO Report, at p. 29.

⁴⁸ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

Loss of Benefit of the Bargain

141. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its services, under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Injunctive Relief is Necessary to Protect Against Future Data Breaches

142. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

143. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

144. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach for which Defendant Navvis & Company, LLC provided notice to Plaintiff and other Class Members beginning on or around December 29, 2023 (the "Class").

145. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

146. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

147. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

148. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class

Members that their Private Information had been compromised;

- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

149. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

150. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

151. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no

disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

152. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

153. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action

alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

154. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, including its privacy policy, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

155. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

156. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Petition.

157. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

158. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;
- c. Whether Defendant failed to comply with its own policies and applicable laws,

regulations, and industry standards relating to data security;

- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and
- i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I **NEGLIGENCE**

159. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

160. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

161. Upon Defendant accepting and storing the Private Information of Plaintiff and Class Members in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected.

162. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendant's duties included the

responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

163. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

164. Defendant owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

165. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA and the FTC Act, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

166. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

167. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair

practice of failing to use reasonable measures to protect confidential data.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either acquires, maintains, or stores.

169. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information, as alleged and discussed above.

170. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

171. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

172. The imposition of a duty of care on Defendant to safeguard the Private Information they maintained is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

173. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time

incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

174. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach in an amount to be determined at trial.

175. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

176. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

177. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

178. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

179. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

180. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.” *See* definition of encryption at 45 C.F.R. § 164.304.

181. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff’s and Class Members’ Private Information.

182. Defendant’s failure to comply with applicable laws and regulations constitutes negligence per se.

183. But for Defendant’s wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

184. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant’s breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant’s breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

185. As a direct and proximate result of Defendant’s negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial “out of pocket” costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time

incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance, and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

186. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach to be determined at trial.

187. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

188. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

189. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

190. In its Privacy Policy, Defendant represented that it would not disclose Plaintiff's and Class Members' Private Information to unauthorized third-parties.

191. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

192. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any Private Information that it was no longer required to maintain.

193. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

194. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices.

195. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

196. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that they were required to reasonably safeguard the Private Information from unauthorized access or disclosure.

197. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, the FTC Act, and were consistent with industry standards.

198. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

199. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their

information reasonably secure.

200. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

201. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

202. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

203. As a direct and proximate result of Defendant's breach of the implied promises, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained incidental and consequential damages including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) diminution of value of their Private Information; (g) future costs of identity theft monitoring; (h) and the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

204. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach to be determined at trial.

205. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

206. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

207. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardians of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with Plaintiff and Class Members, in particular, to keep secure their Private Information.

209. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

210. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff's and Class

Members' Private Information.

211. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

212. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

213. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members sustained compensatory damages including (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

214. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

215. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
INVASION OF PRIVACY

(On Behalf of Plaintiff and All Class Members)

216. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

217. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

218. As a result of Defendant's conduct, publicity was given to Plaintiff and Class Members' Private Information, which necessarily includes matters concerning their private life such as PHI.

219. A reasonable person of ordinary sensibilities would consider the publication of Plaintiff's and Class Members' Private Information to be highly offensive.

220. Plaintiff's and Class Members' Private Information is not of legitimate public concern and should remain private.

221. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's

and Class Members' Private Information.

222. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

223. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

224. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

225. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information. Indeed, in acquiring the Private Information, Defendant was then able to charge money for its medical services.

226. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information, which cost savings increased the profitability of the services.

227. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

228. Under the principles of equity and good conscience, Defendant should not be

permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

229. Defendant acquired the monetary benefit, Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

230. Had Plaintiff and Class Members known that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant. Plaintiff and Class Members have no adequate remedy at law.

231. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

232. Furthermore, as a direct and proximate result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

233. Plaintiff and Class Members are entitled to compensatory, consequential, and

nominal damages suffered as a result of the Data Breach.

234. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

235. Moreover, Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT VII
PROMISSORY ESTOPPEL
(On Behalf of Plaintiff and All Class Members)

236. Plaintiff and the Class repeat and re-allege each and every allegation in the Petition as if fully set forth herein.

237. Defendant promised through its Privacy Policy to protect Plaintiff's and Class Members' Private Information.

238. It was foreseeable that Plaintiff and Class Members would reasonably rely on this promise because Defendant is a reputed and established medical services providers with multiple locations.

239. Plaintiff and Class Members, to their substantial detriment, did in fact rely on Defendant's promises as contained in its Privacy Policy.

240. Furthermore, if Defendant had made it known to Plaintiff and Class Members that they would not have safeguarded Plaintiff's and Class Members' Private Information, Plaintiff and Class Members would not have agreed to receive medical services from Defendant.

241. As a direct and proximate result of Defendant's breach of its promises, Plaintiff and Class Members are at current and ongoing risk of identity theft and have suffered incidental and consequential damages including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; (h) future costs of identity theft protection, and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

242. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

243. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VIII
DECLARATORY AND INJUNCTIVE RELIEF

248. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

249. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

250. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

251. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

252. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect patient Private Information.

253. Defendant still possesses the Private Information of Plaintiff and the Class.

254. To Plaintiffs' knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

255. To Plaintiffs' knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

256. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Navvis. The risk of another such breach is real, immediate, and substantial.

257. As described above, actual harm has arisen in the wake of the Data Breach

regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

258. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

259. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Navvis, Plaintiff and Class Members will likely continue to be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

260. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Navvis, thus eliminating the additional injuries that would result to Plaintiff and Class.

261. Plaintiff and Class Members therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;
- d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;
- e. Ordering that Defendant conduct regular database scanning and security checks; and
- f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring Defendant to engage independent third-party security auditors and

- internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
 - ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - x. requiring Defendant to conduct regular database scanning and securing checks;
 - xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
 - xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
 - xiv. requiring Defendant to implement, maintain, regularly review, and revise as

necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;
 - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
 - F. For prejudgment interest on all amounts awarded; and
 - G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: January 8, 2024

Respectfully Submitted,

/s/ Tiffany Marko Yiatras
Tiffany Marko Yiatras, #58197MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com

Joseph M. Lyon*
Kevin M. Cox*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: jlyon@thelyonfirm.com
Email: kcox@thelyonfirm.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class